

SC-900 Study Guide

Microsoft Security, Compliance, and Identity Fundamentals Exam Resource

PURPOSE

The following resources have been assembled to help you prepare for the SC-900 Microsoft Security Fundamentals learning track during Microsoft Certification Week.

Use this guide to understand what knowledge is needed to complete the exam and as a learning tool to help you understand areas where you feel you need additional training. It is not required that you leverage all the resources in this guide to participate in Microsoft Certification Week.

AUDIENCE

All Pax8 Partners

Table of Contents

SC-900: Exam Resources

Microsoft Learn

Access to the exam objectives can be found on Microsoft Learn: https://docs.microsoft.com/en-us/learn/certifications/exams/sc-900

Preparing with an Azure and M365 Subscription

It is highly recommended when preparing for a Microsoft exam, that you have had some level of hands-on experience with the services within the objectives. Microsoft courses have a GitHub repository for labs that are recommended and available to the public.

- Azure Free Trial: Create your Azure free account today | Microsoft Azure
- Suggested Lab Guides: https://github.com/MicrosoftLearning/AZ-900T0x-MicrosoftAzureFundamentals

The lab guides can be found at this link: https://github.com/MicrosoftLearning
Microsoft offers trial subscriptions for both Azure and Microsoft 365

Creating an Azure free subscription

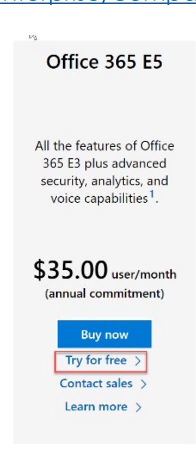
Create your Azure free account today | Microsoft Azure

Creating a Microsoft 365 trial subscription

If you are new to Microsoft 365 and Azure, getting hands on experience is important not just for exam preparation, but also for professional development. If you are getting certified as a way to open doors to new job opportunities, you must understand the administration portals and how to work within them. This book will provide some exercises that will get you familiar with how to work within Microsoft 365 and Azure Active Directory. In order to follow along with the steps, it is recommended that you have a subscription to Microsoft 365 and Azure Active Directory Premium. The steps to create these in as a thirty (30) day trial are provided below.

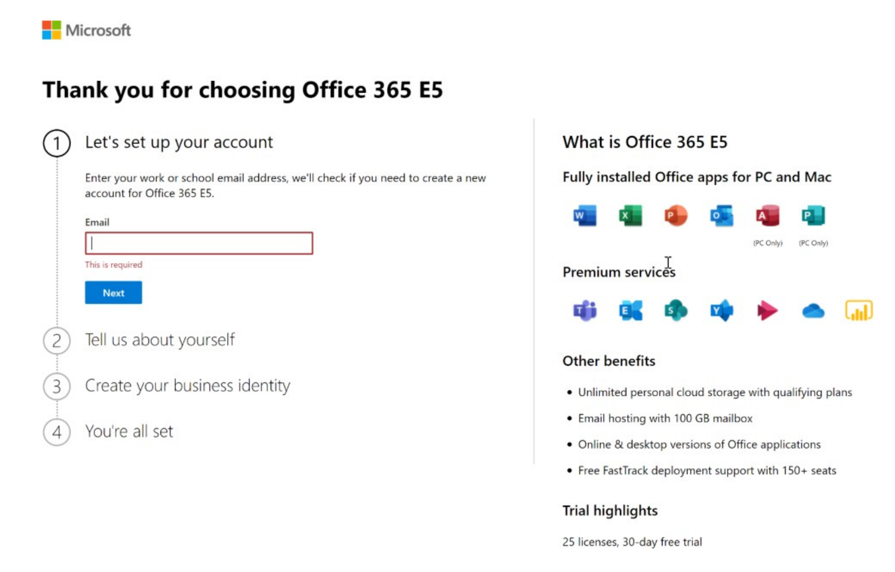
Office 365 or Microsoft 365 trial subscription

Many of the features and capabilities discussed within the exam objectives require an enterprise level license within Microsoft 365. The enterprise licenses are the E3 and E5 licenses. Microsoft offers thirty (30) day trial licenses of these, so as you prepare for the exam, you can create this trial subscription and be able to follow along with the exercises. To get started, navigate to this link and select "try for free" under the Office 365 E5 plan: https://www.microsoft.com/en-us/microsoft-365/enterprise/compare-office-365-plans



Follow the steps to create an account. If you have already created an account previously, you may need to use a different email address to obtain the free trial.





Azure Active Directory Premium subscription
In addition to the Office 365 E5 trial subscription, you will need access to an Azure Active Directory Premium license for many of the advanced identity and access features that are discussed within the exam objectives. The best way to obtain these features is through an Enterprise Mobility + Security E5license. Microsoft also offers this as a thirty (30) day free trial.
To get started, navigate to this link and select "try now" under the Enterprise Mobility + Security E5 plan:
https://www.microsoft.com/en-us/microsoft-365/enterprise-mobility-security/compare-plans- and-pricing
This is an add-on license to Microsoft 365, so you should enter the same email address that you used to sign up for the Office 365 E5 subscription. -

Interactive Guides and Videos

Module 1: Describe the concepts of Security, Compliance, and Identity

- https://edxinteractivepage.blob.core.windows.net/edxpages/Security%20fundamentals/LP01M 02%20Explore%20the%20Service%20Trust%20Portal/index.html
- Module 1, Lesson 1, Topic 2 2.00 Zero Trust (informational) https://www.microsoft.com/enus/videoplayer/embed/RE4J3ms

For more information about the topics covered in this module, see:

- Shared responsibility in the cloud
- Digital signatures
- Azure defense in depth
- Microsoft's Privacy Principles
- Get started with the Microsoft Service Trust Portal
- Microsoft Compliance Manager
- Microsoft Trust Center
- Microsoft Compliance Center Manager documentation
- Free Trial
- Service Trust Portal
- Azure compliance documentation

Module 2: Describe the capabilities of Microsoft Identity and Access Management Solutions

- https://edxinteractivepage.blob.core.windows.net/edxpages/Security%20fundamentals/LP02M 02%20-%20Create%20a%20New%20User%20in%20Azure%20Active%20Directory/index.html



- https://edxinteractivepage.blob.core.windows.net/edxpages/Security%20fundamentals/LP02M 03%20-%20Enable%20SSPR%20in%20Azure%20Active%20Directory/index.html
- https://edxinteractivepage.blob.core.windows.net/edxpages/Security%20fundamentals/LP02M 04%20-%20Create%20a%20Conditional%20Access%20Policy/index.html
- Module 2, Lesson 1, Topic 4 4.50 Azure AD Authentication Fundamentals (informational) https://www.microsoft.com/enus/videoplayer/embed/RE4Kdt9
- Module 2, Lesson 3, Topic 3 1.88 The new sign-in standard: Passwordless authentication(informational) https://www.microsoft.com/enus/videoplayer/embed/RE4zhD7
- Module 2, Lesson 4, Topic 2 1.50 Azure AD Conditional Access (informational) https://www.microsoft.com/enus/videoplayer/embed/RE4INyl
- Module 2, Lesson 5, Topic 3 3.00 AD entitlement management (informational) https://www.microsoft.com/enus/videoplayer/embed/RE4JXQr
- Module 2, Lesson 5, Topic 4 5.50 Privileged identity Management (informational) https://www.microsoft.com/enus/videoplayer/embed/RE4ILbu

For more information about the topics raised in this module, see:

- Protecting your organization against password spray attacks
- Identity protection risks
- Authentication vs authorization
- Identity providers for External Identities
- Compare Active Directory to Azure Active Directory
- What is Azure Active Directory?
- Azure Active Directory Pricing
- Azure AD Licenses
- Azure Active Directory Identity Protection
- Privileged Identity Management
- Azure AD External Identity pricing
- Azure Active Directory External Identities
- Azure Active Directory B2C documentation
- Managed identities
- Services that support managed identities for Azure resources
- What is Azure AD Connect?
- Azure AD registered devices
- Azure AD joined devices
- Hybrid Azure AD joined devices - What are security defaults?
- Licensing requirements for Azure Active Directory self-service password reset
- FIDO2 security keys
- Windows Hello biometrics in the enterprise
- Windows Hello for Business
- Windows Hello for Business Group Policy
- What is Azure Active Directory Authentication?
- Single sign-in overview
- Security Fundamentals - Identity
- Conditional Access
- Security defaults
- Available roles
- Custom administrator roles in Azure AD
- Understand Azure Active Directory role concepts
- Microsoft Identity Manager
- Identity governance
- Dynamic membership rules for groups
- Azure AD Privileged Identity Management
- Azure AD access reviews
- Azure terms of use statements
- Dynamic groups in Azure AD
- Azure entitlement management
- Azure Identity Protection



Module 3: Describe the capabilities of Microsoft Security Solutions

- https://edxinteractivepage.blob.core.windows.net/edxpages/Security%20fundamentals/LP03M 02%20-%20Use%20Azure%20secure%20score%20to%20improve%20your%20security%20posture/inde x.html
- https://edxinteractivepage.blob.core.windows.net/edxpages/Security%20fundamentals/LP03M 04%20-%20Describe%20threat%20protection%20with%20Microsoft%20365/index.html
- https://edxinteractivepage.blob.core.windows.net/edxpages/Security%20fundamentals/LP03M 05%20-%20Explore%20Microsoft%20Secure%20Score/index.html
- Module 3, Lesson 3, Topic 3 9.50 Azure Sentinel (walk-
- through) https://www.microsoft.com/enus/videoplayer/embed/RE4LHLR
- Module 3, Lesson 4, Topic 2 3.50 M365 Defender Overview
- (informational) https://www.microsoft.com/enus/videoplayer/embed/RE4IPYr

MCAS Pillars:

- **Visibility**: detect all cloud services; assign each a risk ranking; identify all users and third-partyapps able to log in
- **Data security**: identify and control sensitive information (DLP); respond to classification labelson content
- **Threat protection**: offer adaptive access control (AAC); provide user and entity behavior analysis(UEBA); mitigate malware
- **Compliance**: supply reports and dashboards to demonstrate cloud governance; assist efforts toconform to data residency and regulatory compliance requirements
- Module 3, Lesson 5, Topic 5 4.20 M365Defender-Incident (walk-through) https://www.microsoft.com/enus/videoplayer/embed/RE4J3mt
- Module 3, Lesson 6, Topic 3 8.36 Explore endpoint security (walk-through) https://www.microsoft.com/en-us/videoplayer/embed/RE4LTlu

To find out more about any of the topics covered in this module, go to:

- Network Security Groups
- Azure DDoS Protection Standard overview
- Azure Firewall
- Azure Bastion
- Web Application firewall
- Encryption
- Spreadsheet showing a walkthrough for the Security Center unit
- Azure Security Center
- Azure secure score
- Azure Defender
- Cloud security posture management and secure score controls
- Security baselines
- Integrated threat protection with SIEM and XDR
- Microsoft delivers unified SIEM and XDR to modernize security operations
- Azure Sentinel and SIEM
- What is Azure Sentinel?
- Azure Sentinel pricing
- Microsoft 365 Defender
- Microsoft Defender for Identity, Defender for Office 365, and Defender for Endpoint
- What is cloud app security
- MCAS and Office 365 Cloud App Security
- Getting started with MCAS
- Overview of the Microsoft 365 security center
- Microsoft Secure Score
- Secure Score in Azure Security Center
- Monitor and view reports in the Microsoft 365 security center
- Incidents overview in Microsoft 365 Defender
- Azure Security Center Documentation
- Microsoft Intune is an MDM and MAM provider for your devices
- Interactive guide: manage devices with Microsoft Endpoint Manager
- Manage endpoint security in Microsoft Intune
- What is Azure role-based access control?



- [Common ways to use Microsoft Intune]
- [Azure RBAC documentation]

Module 4: Describe the capabilities of Microsoft Compliance Solutions

- Module 4, Lesson 1, Topic 4 1.50 Compliance Manager
  https://www.microsoft.com/enus/videoplayer/embed/RE4FGYZ
- Module 4, Lesson 2, Topic 3 4.35 Data Classification in the M365 Compliance Center (walk- through)
  https://www.microsoft.com/enus/videoplayer/embed/RE4vx8x
- Module 4, Lesson 3, Topic 3 7.00 Detect Workplace Harassment & Respond - Communication Compliance in Microsoft 365 (walk-through)
  https://www.microsoft.com/enus/videoplayer/embed/RE4xlaF
- Module 4, Lesson 3, Topic 5 5.70 Privileged Access Management (walk-through)
  https://www.microsoft.com/enus/videoplayer/embed/RE4xqtC
- Module 4, Lesson 6, Topic 5 1.80 Cloud adoption framework video (informational)
  https://www.microsoft.com/enus/videoplayer/embed/RE4tyz

To find out more about any of the topics covered in this module, go to:

- Explore the Microsoft compliance center
- Microsoft 365 compliance center
- Compliance Manager frequently asked questions
- Microsoft Compliance Manager
- Reduce risk with Microsoft Compliance Manager
- Azure compliance documentation
- Know your data - data classification overview
- Get started with content explorer
- Learn about sensitivity labels
- Get started with activity explorer
- Learn about retention policies and retention labels
- Microsoft Information Governance in Microsoft 365
- Learn about records management in Microsoft 365
- Insider risk management in Microsoft 365
- eDiscovery
- Alt-text=Privileged access management
- Customer Lockbox in Office 365
- Get started with communication compliance
- eDiscovery - Microsoft 365 Compliance
- Search for content - Microsoft 365 Compliance
- Get started with core eDiscovery cases in Microsoft 365 - Microsoft 365 Compliance
- Overview of the Advanced eDiscovery solution in Microsoft 365 - Microsoft 365 Compliance
- Search the audit log in the compliance center
- Microsoft 365 compliance center
- Advanced Audit in Microsoft 365
- Turn audit log search on or off
- API Throttling
- Lock resources to prevent unexpected changes
- What is Azure Resource Manager
- What is Azure Blueprints?
- What is the Microsoft Cloud Adoption Framework for Azure?

Microsoft Documents by Objective Area

Describe the Concepts of Security, Compliance, and Identity (5-10%)

Describe security methodologies

- Describe the Zero-Trust methodology
  - Zero Trust Deployment Center

        - Zero Trust Security – microsoft.com
        - Zero-trust methodology
- Describe the shared responsibility model
    - Shared responsibility in the cloud
- Define defense in depth
    - Describe defense in depth

Describe security concepts

- Describe common threats
    - Understanding malware & other threats
- Describe encryption
    - Azure encryption overview
    - Describe ways encryption hashing and signing can secure your data

Describe Microsoft Security and compliance principles

- Describe Microsoft's privacy principles
    - Microsoft Privacy Principles | Microsoft Trust Center
- Describe the offerings of the service trust portal
    - Get started with the Microsoft Service Trust Portal

Describe the capabilities of Microsoft Identity and Access Management Solutions (25- 30%)

Define identity principles/concepts

- Define identity as the primary security perimeter
    - Azure Identity Management and access control security best practices
- Define authentication
    - What is Azure Active Directory authentication?
- Define authorization
    - Authentication vs. authorization
- Describe what identity providers are
    - Identity and access management
    - Identity Providers for External Identities
- Describe what Active Directory is
    - Active Directory Domain Services Overview
- Describe the concept of Federated services
    - Active Directory Federation Services in Azure
- Define common Identity Attacks
    - Azure AD Identity Protection

Describe the basic identity services and identity types of Azure AD

- Describe what Azure Active Directory is
    - What is Azure Active Directory?
- Describe Azure AD identities (users, devices, groups, service principals/applications)
    - What are managed identities for Azure resources?
    - Manage app and resource access using Azure Active Directory groups
    - Securing service principals
- Describe what hybrid identity is
    - What is hybrid identity with Azure Active Directory?
- Describe the different external identity types (Guest Users)
    - What are External Identities in Azure Active Directory?

Describe the authentication capabilities of Azure AD

- Describe the different authentication methods
    - What is Azure Active Directory authentication?
    - What authentication and verification methods are available in Azure ActiveDirectory?

- Describe self-service password reset
    - Tutorial: Enable users to unlock their account or reset passwords using AzureActive Directory self-service password reset
- Describe password protection and management capabilities
    - Eliminate bad passwords using Azure Active Directory Password Protection
    - Enforce on-premises Azure AD Password Protection for Active Directory DomainServices
- Describe Multi-factor Authentication
    - How it works: Azure AD Multi-Factor Authentication
- Describe Windows Hello for Business
    - Windows Hello for Business Overview

Describe access management capabilities of Azure AD

- Describe what conditional access is
    - What is Conditional Access?
- Describe uses and benefits of conditional access
        - What is Conditional Access?
    - Describe the benefits of Azure AD roles
    - Azure AD built-in roles
    - Overview of role-based access control in Azure Active Directory

Describe the identity protection & governance capabilities of Azure AD

- Describe what identity governance is
    - What is Azure AD Identity Governance?
- Describe what entitlement management and access reviews is
    - What are Azure AD access reviews?
- Describe the capabilities of PIM
    - What is Azure AD Privileged Identity Management?
- Describe Azure AD Identity Protection
    - What is Identity Protection?

Describe the capabilities of Microsoft Security Solutions (30-35%)

Describe basic security capabilities in Azure

- Describe Azure Network Security groups
    - Network security groups
- Describe Azure DDoS protection
    - Azure DDoS Protection Standard overview
- Describe what Azure Firewall is
    - What is Azure Firewall?
- Describe what Azure Bastion is
    - What is Azure Bastion?
- Describe what Web Application Firewall is
    - What is Azure Web Application Firewall on Azure Application Gateway?
- Describe ways Azure encrypts data
    - Azure encryption overview
    - Data encryption in Azure

Describe security management capabilities of Azure

- Describe the Azure Security center
    - What is Azure Security Center?
- Describe Azure Secure score
    - Secure score in Azure Security Center
- Describe the benefit and use cases of Azure Defender – previously the cloud workloadprotection platform (CWPP)
    - Introduction to Azure Defender



- Describe Cloud security posture management (CSPM)
    - Function of cloud security posture management
- Describe security baselines for Azure
    - Security baselines for Azure

Describe security capabilities of Azure Sentinel

- Define the concepts of SIEM, SOAR, XDR
    - What is Azure Sentinel?
- Describe the role and value of Azure Sentinel to provide integrated threat protection
    - Quickstart: Get started with Azure Sentinel

Describe threat protection with Microsoft 365 Defender (formerly Microsoft Threat Protection)

- Describe Microsoft 365 Defender services
    - Microsoft 365 Defender
- Describe Microsoft Defender for Identity (formerly Azure ATP)
    - What is Microsoft Defender for Identity?
- Describe Microsoft Defender for Office 365 (formerly Office 365 ATP)
    - Microsoft Defender for Office 365 in the Microsoft 365 security center
- Describe Microsoft Defender for Endpoint (formerly Microsoft Defender ATP)
    - Redirecting accounts from Microsoft Defender for Endpoint to the Microsoft365 security center
- Describe Microsoft Cloud App Security
    - Microsoft Cloud App Security overview

Describe security management capabilities of Microsoft 365

- Describe the Microsoft 365 Security Center
    - The unified Microsoft 365 security center overview
- Describe how to use Microsoft Secure Score
    - Microsoft Secure Score
- Describe security reports and dashboards
    - Smart reports and insights in the Security & Compliance Center
- Describe incidents and incident management capabilities
    - Manage incidents in Microsoft 365 Defender

Describe endpoint security with Microsoft Intune

- Describe what Intune is
    - Microsoft Intune is an MDM and MAM provider for your devices
- Describe endpoint security with Intune
    - Manage endpoint security in Microsoft Intune
- Describe the endpoint security with the Microsoft Endpoint Manager admin center
    - Manage endpoint security in Microsoft Intune

Describe the Capabilities of Microsoft Compliance Solutions (25-30%)

Describe the compliance management capabilities in Microsoft

- Describe the compliance center
    - Microsoft 365 compliance center
- Describe compliance manager
    - Microsoft Compliance Manager
- Describe use and benefits of compliance score
    - Compliance score calculation

Describe information protection and governance capabilities of Microsoft 365

- Describe data classification capabilities
    - Microsoft Information Protection in Microsoft 365
    - Know your data – data classification overview



- Describe the value of content and activity explorer
    - Get started with activity explorer
- Describe sensitivity labels
    - Learn about sensitivity labels
- Describe Retention Policies and Retention Labels
    - Get started with retention policies and retention labels
- Describe Records Management
    - Learn about records management in Microsoft 365
- Describe Data Loss Prevention
    - Overview of data loss prevention

Describe insider risk capabilities in Microsoft 365

- Describe Insider risk management solution
- Learn about insider risk management in Microsoft 365
- Describe communication compliance
- Learn about communication compliance in Microsoft 365
- Describe information barriers
- Learn about information barriers in Microsoft 365
- Describe privileged access management
- Privileged access management in Microsoft 365
- Describe customer lockbox
- Customer Lockbox in Office 365

Describe the eDiscovery capabilities of Microsoft 365

- Describe the purpose of eDiscovery
    - eDiscovery solutions in Microsoft 365
- Describe the capabilities of the content search tool
    - Content Search
- Describe the core eDiscovery workflow
    - Get started with Core eDiscovery
- Describe the advanced eDisovery workflow
    - Overview of Microsoft 365 Advanced eDiscovery

Describe the audit capabilities in Microsoft 365

- Describe the core audit capabilities of M365
    - Search the audit log in the compliance center
- Describe purpose and value of Advanced Auditing
    - Advanced Audit in Microsoft 365

Describe resource governance capabilities in Azure

- Describe the use of Azure Resource locks
    - Lock resources to prevent unexpected changes
    - Azure Resource Locks
- Describe what Azure Blueprints is
    - What is Azure Blueprints?
- Define Azure Policy and describe its use cases
    - What is Azure Policy?
    - Azure Policy
- Describe cloud adoption framework
    - What is the Microsoft Cloud Adoption Framework for Azure?